УДК 681.3.06

Паламарчук Н.А. (ВІТІ НТУУ „КПІ”)
к.т.н. Хлапонін Ю.І. (ВІТІ НТУУ „КПІ”)
к.т.н. Овсяннiков В.В. (ВІТІ НТУУ „КПІ”)

СУЧАСНИЙ СТАН НОРМАТИВНО-ПРАВОВОЇ БАЗИ В ГАЛУЗІ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

Проаналізовано сучасний стан нормативно-правової бази в галузі технічного захисту інформації, наведено деякі протиріччя, які існують в термінології та вимогах нормативно-правових актів з технічного захисту інформації. За результатами дослідження зроблено висновок, що діюча нормативна база потребує доопрацювання та впровадження єдиних підходів в даній галузі.

***Паламарчук Н.А., Хлапонин Ю.И., Овсянников В.В. Современное состояние нормативной базы в отрасли технической защиты информации**. Проанализировано современное состояние нормативно-правовой базы в области технической защиты информации, приведены некоторые противоречия, которые существуют в терминологии и требованиях нормативных документов системы технической защиты информации. По результатам исследования сделан вывод о том, что действующая нормативная база требует доработки и внедрения единых подходов в данной отрасли.*

***N.Palamarchuk, Y.Khlaponin, V.Ovsjannikov The modern state of normative legal base in the area of technical protection of information.** The modern state of normative legal base in area of technical protection of information is analysed, some contradictions that exist in terminology and requirements of normative documents of the system of technical protection of information, are brought. On results of research is drawn a conclusion that an operating normative base requires a revision and introduction of single approaches in this area.*

***Ключові слова**: інформація з обмеженим доступом (ІзОД). інформаційно-телекомунікаційна система (ІТС), інформаційна система (ІС), автоматизована система (АС), обчислювальна система (ОС), комп'ютерна система (КС), технічний захист інформації (ТЗІ), комплексна система захисту інформації (КСЗІ), комплекс засобів захисту (КЗЗ).*

Технічний захист інформації займає особливо важливе місце в загальному комплексі заходів щодо забезпечення національної безпеки України в інформаційній сфері та безпосередньо призначений для забезпечення організаційними, інженерними та технічними заходами, методами і засобами конфіденційності, цілісності та доступності інформації, яка обробляється в інформаційно-телекомунікаційних системах (ІТС), циркулює на об'єктах інформаційної діяльності та становить державну та іншу встановлену законом таємницю, віднесена до службової інформації або є відкритою, вимога щодо захисту якої встановлена законом. Система технічного захисту інформації як кожна організаційно-технічна система складається з трьох основних компонентів: нормативно-правової бази, організаційної інфраструктури та матеріально-технічної бази.

Безперечним є те, що головною складовою системи, яка впливає на дві інші є нормативно-правова база, оскільки саме вона визначає її правові та організаційні засади, норми та вимоги з технічного захисту інформації. В цілому, створена в Україні нормативно-правова база забезпечує функціонування системи технічного захисту інформації.

Але справа в тім, що в Україні є дійсними (діючими) як державні стандарти та нормативні документи ще радянського періоду так і нормативно-правові акти, видані вже Адміністрацією Держспецзв'язку України (або ще їх попередниками). Різноманітність цих документів, неузгодженість між собою окремих положень, що в них містяться, не дозволяє у повному обсязі реалізувати єдину політику в проектуванні та експлуатації систем технічного захисту інформації, ускладнює роботу виконавців та експертів, а отже створює передумови для можливих невиправданих інтелектуальних й економічних витрат.

Вимоги зазначених документів в деяких питаннях можуть суперечити один одному. Прикладом різного тлумачення нормативної бази може бути наступне.

Так, в [1] *дається визначення автоматизованої системи (АС – automated system) як організаційно-технічної системи, що реалізує інформаційну технологію і об'єднує обчислювальну систему, фізичне середовище, персонал і інформацію, яка обробляється. Дане визначення не відповідає* [2]*, який встановлює терміни та визначення в галузі АС.*

Законом України [3] вводиться поняття інформаційна (автоматизована) система – організаційно-технічна система, в якій реалізується технологія обробки інформації з використанням технічних і програмних засобів.

Виходячи з цих визначень, виникає питання чи входить до складу інформаційної системи обчислювальна система (ОС), фізичне середовище, персонал і інформація, яка обробляється як вказано в [1].

В [4] подано терміни та визначення інформаційної, телекомунікаційної та інтегрованої систем як видів автоматизованих систем.

Поняття інформаційної системи викладене як організаційно-технічна система, що реалізує технологію обробки інформації за допомогою засобів обчислювальної техніки та програмного забезпечення, тобто поняття обчислювальної системи [1] або обчислювальної техніки [4] в складі ІС знову має місце.

Вказано також, що під інформаційно-телекомунікаційною системою (ІТС) розуміється будь-яка система, яка відповідає одному з трьох наведених вище видів автоматизованих систем.

Але, як може інформаційна (автоматизована) система бути ІТС не виконуючи при цьому функції ,,обміну інформацією шляхом передавання, випромінювання або приймання її у вигляді сигналів, знаків, звуків, рухомих або нерухомих зображень чи в інший спосіб” [4]? Визначення ж класів АС в [5] стає не актуальним (некоректним), з введенням Закону [3].

Діючим є також [6], в якому використовується поняття комп’ютерної системи (КС), яка в найбільш загальному випадку являє собою АС або її частину.

Зрозуміло, що починаючи вже з ключових термінів (АС, ІС, ІТС) немає однозначних визначень цих понять, діюча нормативна база з ТЗІ потребує доопрацювання та впровадження єдиної термінології. Деякі автори навіть вважають, що захисту інформації в ІТС властива специфічна термінологія, професійна та жаргонна [7]. Насправді ж, термінологія має відображати концептуальні підходи до вирішення проблеми. Таким чином, роблячи посилання на те чи інше визначення (термін) доцільно вказувати згідно яких нормативно-правових документів вживаються визначення в тому чи іншому випадку.

Наступна думка, в [1] надається визначення політики безпеки інформації (information security policy) як сукупності законів, правил, обмежень, рекомендацій, інструкцій тощо, які регламентують порядок обробки інформації. В [4] визначено, що політика безпеки розробляється згідно з положеннями [6] та рекомендаціями [8]. Політику безпеки рекомендується оформляти у вигляді окремого документа Плану захисту. В той же час згідно [8] політика безпеки інформації в АС має бути окремим розділом Плану захисту інформації в АС та враховувати вимоги п. 5.6 Додатку [8], який, в свою чергу, посилається на [4]. В результаті, взаємні посилання з одного документа на інший ускладнюють роботу виконавців робіт з ТЗІ.

Що ж стосується світового досвіду то, на міжнародному рівні політика безпеки розглядається набагато ширше. Як приклад, міжнародні стандарти в області інформаційної безпеки, частково в *ISO/IEC 17799:2000*. Керування інформаційною безпекою – Інформаційні технології [9], який був прийнятий в 2000 р. та з часом переглядався і доповнювався (*ISO/IEC 27001:2005* [10]. Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Вимоги). Згідно міжнародних стандартів відпрацьовується політика безпеки підприємства, яка включає в тому числі і інформаційну безпеку. Також надається перелік документів, які повинні бути відпрацьовані разом з політикою безпеки (положення, інструкції, рекомендації та ін.).

В цілому, ***політика безпеки*** – сукупність програмних, апаратних, організаційних, адміністративних, юридичних, фізичних заходів, методів, засобів, правил і інструкцій, чітко регламентуючих всі аспекти діяльності компанії, включаючи інформаційну систему і, забезпечуючи їхню безпеку. Політика безпеки є одним з найважливіших, життєво важливих документів компанії.

Переваги для установ, організацій, підприємств, які будують системи управління інформаційною безпекою відповідно до міжнародних стандартів та в подальшому отримують сертифікати на відповідність ISO/IEC 27001: 2005 наступні:

– підвищення керованості та надійності;

– підвищення захищеності ключових напрямків діяльності;

– спрощення процедури виходу на міжнародний рівень;

– міжнародне визнання та підвищення авторитету;

– систематизація процесів управління безпекою інформації та ін.

Загалом, міжнародні стандарти в області інформаційної безпеки в Україні не є обов’язковими для виконання та носять лише рекомендаційний характер, хоча, наприклад, Національним банком України міжнародний стандарт [10] прийнятий в 2010 році в якості галузевого *ГСТУ СУІБ 1.0/ISO/IEC 27001:2010*.

Як бачимо із зазначеного, політика безпеки є одним із першочергових документів, які розробляються в установі, організації, на підприємстві, щодо інформаційної безпеки, а наприклад, план захисту інформації відпрацьовується на її основі. Це суттєво відрізняється від положень нормативних документів системи технічного захисту інформації в Україні, в яких політиці безпеки надається не достатня увага, хоча згідно п 5.1 Додатку [8] політика безпеки інформації в АС є частиною загальної політики безпеки організації і повинна успадковувати основні її принципи. На практиці, в Україні розробка політики безпеки організації зводиться до відпрацювання вимог до політики безпеки інформації в АС, складовими частинами якої мають існувати політики забезпечення конфіденційності, цілісності і доступності оброблюваної інформації [6].

На думку фахівців, бажано мати типову політику безпеки для окремого відомства (міністерства), що дасть можливість запобігти непорозумінням та прискорити виконання робіт зі створення КСЗІ в ІТС.

В той же час в [11] п. 19 визначається, що План захисту інформації в системі містить:

– завдання захисту, класифікацію інформації, яка обробляється в системі, опис технології обробки інформації;

– визначення моделі загроз для інформації в системі;

– основні вимоги щодо захисту інформації та правила доступу до неї в системі;

– перелік документів, згідно з якими здійснюється захист інформації в системі;

– перелік і строки виконання робіт службою захисту інформації.

Як бачимо, мова про *політику безпеки* тут вже не ведеться.

Далі виникає питання стосовно визначення моделі загроз для інформації. Чи слід розуміти, що мова йде про розроблення окремого документа згідно з вимогами [12]. Але як відомо, відповідно до [12] розробляється модель загроз для інформації з обмеженим доступом (загрози від витоку ІзОД технічними каналами).

В [6] виділяють два основних напрями ТЗІ в АС – це захист АС і оброблюваної інформації від несанкціонованого доступу та захист інформації від витоку технічними каналами (оптичними, акустичними, захист від витоку каналами побічних електромагнітних випромінювань і наведень). Виникає питання, якщо в АС обробляється відкрита інформація, то згідно [11] вимоги до захисту інформації від витоку технічними каналами не є обов’язковими, і висуваються у відповідності до рішення власника (розпорядника) інформації. Вимоги щодо захисту інформації від несанкціонованих дій, у тому числі від комп’ютерних вірусів, висуваються для всіх систем, відповідно, модель загроз для інформації відпрацьовується згідно вимог [6]. Загрози оброблюваної в АС інформації залежать від характеристик ОС, фізичного середовища, персоналу і оброблюваної інформації. Загрози можуть мати або об’єктивну природу, наприклад, зміна умов фізичного середовища (пожежі, повені і т. ін.) чи відмова елементів ОС, або субє’ктивну, наприклад, помилки персоналу чи дії зловмисника. Із всієї множини способів класифікації загроз найпридатнішою для аналізу є класифікація загроз за результатом їх впливу на інформацію, тобто порушення конфіденційності, цілісності і доступності інформації [6].

Як порушник розглядається особа, яка може одержати доступ до роботи з включеними до складу КС засобами. Порушники класифікуються за рівнем можливостей, що надаються їм штатними засобами КС. Припускається, що в своєму рівні порушник – це фахівець вищої кваліфікації, який має повну інформацію про КС і КЗЗ.

Така класифікація порушників є корисною для використання в процесі оцінки ризиків, аналізу вразливості системи, ефективності існуючих і планових заходів захисту.

Відповідно до вимог [4] визначаються потенційні загрози для інформації і розробляються модель загроз та модель порушника. Побудова моделей здійснюється відповідно до положень [6, 8, 12]. Модель загроз для інформації та модель порушника рекомендується оформляти у вигляді окремих документів (або поєднаних в один документ) Плану захисту. Моделі є вихідними даними для розроблення політики безпеки і проектування системи захисту взагалі.

Проектування систем захисту інформації починається з відпрацювання технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі.

В технічному завданні на КСЗІ, висуваючи вимоги до захисту АС і оброблюваної інформації від несанкціонованого доступу необхідно встановити функціональний профіль захищеності цієї інформації згідно [5, 13] (на основі моделі загроз для інформації).

З точки зору забезпечення безпеки інформації АС (КС) або КЗЗ можна розглядати як набір функціональних послуг. Кожна послуга являє собою набір функцій, що дозволяють протистояти деякій множині загроз.

Функціональна послуга буде вважатися реалізованою, якщо вона відповідає критеріям оцінки захищеності цієї інформації згідно [13]. Критерії є методологічною базою для визначення вимог з захисту інформації в комп’ютерних системах від несанкціонованого доступу; створення захищених комп’ютерних систем і засобів захисту від несанкціонованого доступу; оцінки захищеності інформації в комп’ютерних системах і їх придатності для обробки критичної інформації (інформації, що вимагає захисту).

Вимоги до функціональних послуг розбиті на чотири групи, кожна з яких описує вимоги до послуг, що забезпечують захист від загроз одного з чотирьох основних типів: конфіденційності, цілісності, доступності та спостережності (відповідно до основних властивостей інформації та АС).

Згідно з [6, 13], кожна послуга може включати декілька рівнів. Чим вище рівень послуги, тим повніше забезпечується захист від певного виду загроз. *Для кожної послуги повинна бути розроблена політика безпеки, яка буде реалізована КС.* Політика безпеки має визначати, до яких об’єктів застосовується послуга. Ця визначена підмножина об’єктів називається захищеними обє’ктами відносно даної послуги.

Як зазначалося, вже під час розробки технічного завдання на створення КСЗІ в АС [14] має бути вказаний функціональний профіль захищеності, який передбачається реалізувати. Стандартний функціональний профіль захищеності являє собою перелік мінімально необхідних рівнів послуг, які повинен реалізовувати КЗЗ обчислювальної системи АС, щоб задовольняти певні вимоги щодо захищеності інформації, яка обробляється в даній АС.

Профіль може бути або вибраний із профілів, описаних в [5] на підставі класу АС або визначений як упорядкована сукупність рівнів послуг в результаті проведення аналізу загроз та оцінки ризиків згідно з вимогами зазначеного документа.

Знову знаходимо деяке протиріччя. Так, в [5] для стандартних функціональних профілів захищеності не вимагається зв’язаної з ними *політики безпеки*. В той час в [6, 13] вказується, що політика безпеки повинна бути розроблена для кожної послуги, з яких, власне, і формується профіль. На практиці, виконавці робіт з ТЗІ при розробці політики безпеки інформації в АС (зауважте, саме інформації в АС, а не політики безпеки організації, на що автори вказували вище) під час вибору функціонального профілю захищеності та висування вимог до функціональних послуг безпеки оперують поняттям *політики* конкретної *послуги*, наприклад, політика адміністративної конфіденційності (КА-2) або політика відновлення після збоїв (ДВ-1) та ін. Виникає питання, чи є набір політик конкретних послуг

складовою вимог, які повинні бути реалізовані згідно політики безпеки. Складається враження, що набір політик конкретних послуг згідно [5, 13] розглядається відокремлено від вимог до розроблення політики безпеки інформації в АС [6, 8].

Таким чином, видно, що виконавець робіт з ТЗІ має керуватися нормативно-правовими документами з захисту інформації, які мають взаємні посилання один на одного, в одному випадку мають дещо відмінні вимоги, а в іншому дублюють один одного. Це ускладнює роботу щодо створення систем захисту інформації, призводить до відпрацювання відповідних організаційно-розпорядчих документів, які цілими розділами (або частинами) повторюють один одного та невиправданих витрат часу виконавцем робіт з ТЗІ та фінансових витрат замовника, і як наслідок може зводитись до формального виконання вимог з захисту інформації.

Впроваджені в останні роки закони, що стосуються інформації та її захисту, а також внесення змін та доповнень до діючих потребує вжиття певних заходів з метою приведення нормативної бази системи технічного захисту інформації у відповідність до вимог цих законів. Діюча нормативна база з питань ТЗІ потребує доопрацювання з метою підвищення ефективності захисту інформації, впровадження єдиного порядку виконання заходів та упорядкування процедури. І в будь-якому разі, без якісної нормативно-правової бази навряд чи можливе ефективне впровадження інших (організаційних та технічних) заходів захисту інформації.

ЛІТЕРАТУРА

1. НД ТЗІ 1.1-003-99. Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу.

2. ДСТУ 2226-93. Автоматизовані системи. Терміни та визначення.

3. Закон України від 5.07.1994 року № 80/94-ВР. Про захист інформації в інформаційно-телекомунікаційних системах.

4. НД ТЗІ 3.7-003-05. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі.

5. НД ТЗІ 2.5-005 -99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу.

6. НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу.

7. Грайворонський М.В. Безпека інформаційно-комунікаційних систем / М.В.Грайворонський, О.М. Новіков. – Київ, Видавнича група BHV, 2009. – 608 с.

8. НД ТЗІ 1.4-001-2000. Типове положення про службу захисту інформації в автоматизованій системі.

9. ISO 17799:2000. Керування інформаційною безпекою – Інформаційні технології.

10. ISO/IEC 27001:2005. Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Вимоги.

11. Постанова Кабінету Міністрів України від 29 березня 2006 р. N 373. Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах.

12. НД ТЗІ 1.6-003 -04. Створення комплексів технічного захисту інформації на об’єктах інформаційної діяльності. Правила розроблення, побудови, викладення та оформлення моделі загроз для інформації.

13. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу.

14. НД ТЗІ 3.7-001-99 Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі.

15. ДСТУ 3396.2-97. Захист інформації. Технічний захист інформації. Терміни та визначення.